ENERGY ASSURANCE TECHNOLOGIES

Project Fact Sheet

Cyber Security for Utility Operations

Benefits

- Develops fundamental tools needed to identify, authorize and validate the source of data or access to data on SCADA systems
- Provides key management tailored to needs of SCADA systems
- Provides cryptographic security in SCADA retrofit solutions
- Provides secure authentication of maintenance ports
- Supports a future embedded solution for new Intelligent Electronic Devices

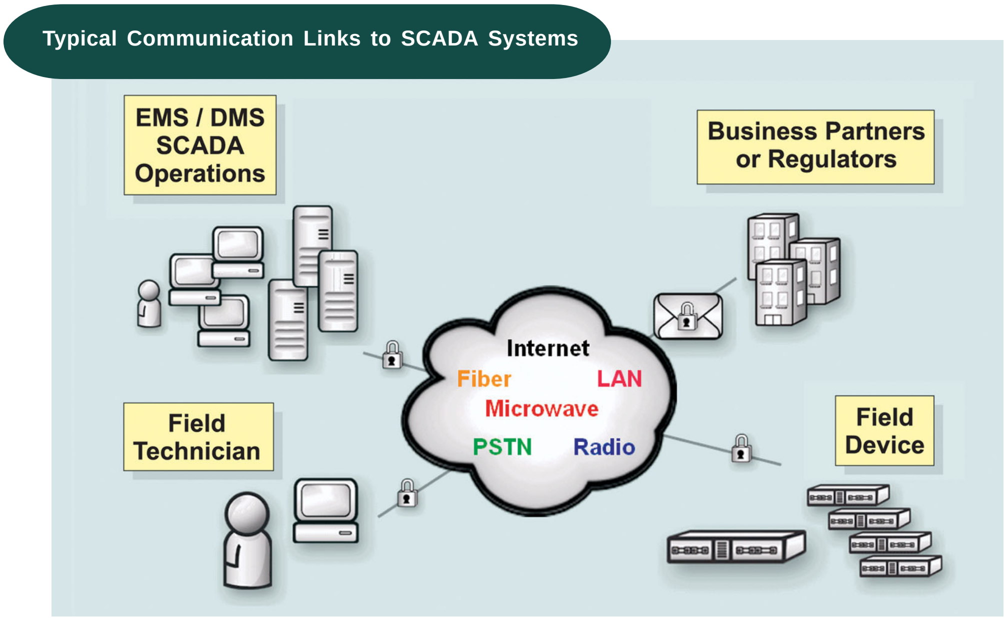
Applications

The critical technology components developed and demonstrated by this project will advance a comprehensive, rather than a piecemeal, solution to SCADA system security and provide a solution that will be more efficient and cost effective. The nearer term applications will be retrofit solutions to legacy SCADA systems in the utility industry, including electric, natural gas, water and waste water utilities. Longer term, the project work will advance the development of new hardware and software designs for new SCADA systems and components, such as embedded solutions for Intelligent Electronic Devices, for these same industries. These solutions could also be applied to any SCADA system, regardless of industry, that has numerous communication links, field devices, and users.

Advanced cryptographic techniques will be integrated into encryption, authentication, and key management products to provide comprehensive, cost effective cyber security

The utility industry increasingly relies upon Supervisory Control and Data Acquisition (SCADA) systems and Energy Management Systems (EMS) in the performance of utility operations. Initial SCADA and EMS systems operated in closed communication loops accessible only by their utility owners. Security protocols were not then deemed necessary. However, increasingly these systems now use the same public telecommunications switching networks and the Internet available to the public for SCADA and EMS systems communications. Generally, these SCADA and EMS resources were designed with minimal security features to protect against cyber intrusions and details of these security features are usually obtainable in the public domain. This situation makes many critical energy infrastructure SCADA systems potentially vulnerable to cyber intrusion. Retrofit solutions for many older legacy SCADA systems are often hampered by inherent system limitations. No comprehensive cost effective cyber security solution currently exists. This project seeks to advance the achievement of such a solution.

Recent cryptography R&D has enabled advances in algorithms, hardware designs, and key management for efficient, low-power authentication and encryption. These results will be integrated with the project industrial partners' initial cryptographic system level design. A proof-of concept design for SCADA critical technology components will be developed and will then be demonstrated at the facilities of a project utility partner.


Typical Communication Links to SCADA Systems

This project will advance SCADA cyber security for utilities by integrating advanced cryptographic techniques into new products to cost effectively protect SCADA communication links.

Project Description

The project will identify and integrate into a system design the critical technologies that must be demonstrated to move towards commercializing products needed for comprehensive and cost effective cyber assurance of SCADA systems. The project focuses on developing technology to provide retrofit solutions for existing legacy SCADA systems that will protect against unauthorized access to the system from the "outside" via SCADA communication links. The technology needed to protect "data at rest" (who has access to the data, how they can use the data, and the controlled time of its use) is well understood and accepted. Requirements to deploy a cost effective solution to protect the "data in transit" is also well understood. Implementation, however, is dependent on a low cost design for three components:

- A secure authentication module is needed to strengthen the access control to device maintenance ports.
- A secure encryption and authentication module is needed to protect data over installed SCADA and EMS communication links.
- A secure management system is needed for key management and distribution.

The project will bring technologies from Sandia together with those from its industry partners to develop these components sufficiently to perform a proof-of-concept demonstration.

Progress and Milestones

This project includes the following milestones:

- Evaluate and update current utility security requirements (1Q/04 [completed])
- Assess and update the project partner's cyber security system designs (2Q/04)
- Integrate state-of-the-art products from Sandia, TecSec, and Mykotronx into a system design (2Q/04)
- Demonstrate a proof-of-concept security system at utility facilities (3Q/04)
- Refine commercialization plan for a cyber security system (3Q/04)

Economic and Commercial Potential

There are over one thousand SCADA systems in operation in electric utilities, each with many remote terminal units (RTUs). Electric utility SCADA systems typically are larger and more complex than in other utilities. A large electric utility can have about 200 communication links and 5,000 RTUs associated with their SCADA system. There are also many SCADA systems in service in other segments of the nation's utility infrastructure (e.g., natural gas, water and waste water utilities). All are candidates for the retrofit solutions being developed in this project.

The economic costs of retrofitting an existing SCADA system with additional cyber security measures must be weighed against the potential losses that can be caused by a successful malicious cyber attack against the system and its perceived likelihood. These losses can include not only disruptions to internal utility operations, but also disruption of service to its customers and, in extreme cases, disruption to the economic activity of a local area or a region. Generally, the utility industry acknowledges that SCADA systems have some vulnerabilities to cyber intrusions. However, the cost and difficulty in implementing additional security measures, particularly for older SCADA systems, is dissuading utilities from making upgrades. Without a more comprehensive and relatively lower cost solution, most utilities are unlikely to embark on a security upgrade to their SCADA systems. By advancing a comprehensive low cost solution, this project can make the business case for SCADA system security upgrades more compelling and, thereby, contribute towards improving the assurance of the U.S. energy infrastructure.

Project Partners

Sandia National Laboratories
Albuquerque, NM

Mykotronx, Inc.
Torrance, CA

TecSec, Inc.
Vienna, VA

OPUS Publishing
Seal Beach, CA

Peoples Energy
Chicago, IL

DTE Energy
Detroit, MI

Interested in joining the partnership, being informed of outcomes, or being a demonstration site? Contact:

Timothy J. Draelos, Ph.D.
Cryptography & Information Systems Surety Department
Sandia National Laboratories
P.O. Box 5800; MS 0785
Albuquerque, NM 87185-0785
Phone/Fax: (505) 844-8698 / 845-7065
Email: tjdrael@sandia.gov

or

David Szucs
U.S. Department of Energy
National Energy Technology Laboratory
626 Cochrans Mill Road
Pittsburgh, PA 15236-0940
Phone: 412-386-4899
Email: szucs@netl.doe.gov

For Program Information, Contact:

Craig Zingman
Program Manager
U.S. Department of Energy
Office of Energy Assurance
1000 Independence Ave, SW
Washington, DC 20585
Phone: 202-586-1043
Email: Craig.Zingman@hq.doe.gov

or

Albert B. Yost II
Business Area Coordinator
U.S. Department of Energy
National Energy Technology Laboratory
3610 Collins Ferry Road
Morgantown, WV 26507-0880
Phone: 304-285-4479
Email: ayost@netl.doe.gov

For Additional Information:

Visit our home page at
www.ea.doe.gov

Office of Energy Assurance
U.S. Department of Energy
Washington, D.C. 20585

March 2004